Attorney Docket No. 324628006US1

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on:

Date: September 16, 2002

By: Sandy Reisman

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: C. Andrew Neff
APPLICATION NO.: 10/038,752
FILED: December 31, 2001
FOR: **DETECTING COMPROMISED BALLOTS**

EXAMINER: Unknown
ART UNIT: 2165
CONF. NO: 6285

Information Disclosure Statement Within Three Months of Application Filing or Before First Action – 37 CFR 1.97(b)

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

1. Timing of Submission

This information disclosure is being filed within three months of the filing date of this application or date of entry into the national stage of an international application or before the mailing date of a first Office action on the merits, whichever occurs last [37 CFR 1.97(b)]. The references listed on the enclosed Form PTO/SB/08A (modified) may be material to the examination of this application; the Examiner is requested to make them of record in the application.

2. Cited Information

□ Copies of the following references are enclosed:

□ All cited references
□ References marked by asterisks
□ The following:

☒ Copies of the following references can be found in parent U.S. Application No. 09/816,869:

☒ All cited references
□ References marked by asterisks
□ The following:

□ The following references are not in English. For each such reference, the undersigned has enclosed (i) a translation of the reference; (ii) a copy of a communication from a foreign patent office or International Searching Authority citing the reference, (iii) a copy of a reference which appears to be an English-language counterpart, or (iv) an English-language abstract for the reference prepared by a third party. Applicant has not verified that the translation, English-language counterpart or third-party abstract is an accurate representation of the teachings of the non-English reference, though, and reserves the right to demonstrate otherwise.

□ All cited references
□ References marked by ampersands
□ The following:

3. Effect of Information Disclosure Statement (37 CFR 1.97(h))

This Information Disclosure Statement is not to be construed as a representation that: (i) a search has been made; (ii) additional information material to the examination of this application does not exist; (iii) the information, protocols, results and the like reported by third parties are accurate or enabling; or (iv) the cited information is, or is considered to be, material to patentability. In addition, applicant does not admit that any enclosed item of information constitutes prior art to the subject invention and specifically reserves the right to demonstrate that any such reference is not prior art.

4. Fee Payment

No fees are believed due. However, should the Commissioner determine that fees are due in order for this Information Disclosure Statement to be considered, the Commissioner is hereby authorized to charge such fees to Deposit Account No. 50-0665.

5. Patent Term Adjustment (37 CFR 1.704(d))

□ The undersigned states that each item of information submitted herewith was cited in a communication from a foreign patent office in a counterpart application and that this communication was not received by any individual designated in 37 C.F.R. § 1.56(c) more than thirty days prior to the filing of this statement. 37 C.F.R. § 1.704(d).

Respectfully submitted,
Perkins Coie LLP

Steven D. Lawrenz
Registration No. 37,376

Correspondence Address:
Customer No. 25096
Perkins Coie LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 583-8888

Please type a plus sign (+) inside this box → +

PTO/SB/08A
Approved for use through 10/31/99. OMB 0651-0031
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	2

COMPLETE IF KNOWN	
Application Number	10/038,752
Confirmation Number	6285
Filing Date	December 31, 2001
First Named Inventor	C. Andrew Neff
Group Art Unit	2165
Examiner Name	
Attorney Docket No.	324628006US1

U.S. PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.	U.S. Patent Document NUMBER	Kind Code (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		5,278,753		Graft, III	1/11/94	
		5,400,248		Chisholm	3/21/95	
		5,495,532		Kilian et al.	2/27/96	
		5,521,980		Brands	5/28/96	
		5,682,430		Kilian et al.	10/28/97	
		5,717,759		Micali	2/10/98	
		5,864,667		Barkan	1/26/99	
		5,878,399		Peralto	3/2/99	

FOREIGN PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.	Foreign Patent Document Office	Number	Kind Code (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
		EP	0 697 776	A2	NEC Corporation	2/21/96		
		EP	0 743 620	A2	NEC Corporation	11/20/96		
		WO	98/14921		Certco, LLC	4/9/98		

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.	T
		Benaloh, J., "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag, Berlin, 1987	
		Benaloh, J., et al., "Distributing the Power of a Government to Enhance the Privacy of Voters", ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986	
		Borrell, Joan et al., "An implementable secure voting scheme", *Computers & Security*, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338	
		Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182	
		Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981	
		Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology – EUROCRYPT 1997, Lecture Notes in Computer Science, Springer-Verlag, 1997.	

EXAMINER	DATE CONSIDERED

* EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Please type a plus sign (+) inside this box → +

PTO/SB/08A
Ap[illegible]d for use through 10/31/99. OMB 0651-0031
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	2	of	2

COMPLETE IF KNOWN	
Application Number	10/038,752
Confirmation Number	6285
Filing Date	December 31, 2001
First Named Inventor	C. Andrew Neff
Group Art Unit	2165
Examiner Name	
Attorney Docket No.	324628006US1

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.	T
		Cramer, R., et al., "Multi-Authority, Secret-Ballot Elections with Linear Work", Advances in Cryptology – EUROCRYPT 1996, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1996	
		Cramer, R., et al., "Proofs of Partial Knowledge and Simplified Design of Cryptology – CRYPTO 1994, Lecture Notes in Computer Science, pp. 174-187, Springer-Verlag, Berlin, 1994	
		Cranor, Lorrie et al., "Sensus: A Security-Conscious Electronic Polling System for the Internet", Proceedings of the Hawaii International Conference on System Sciences, IEEE 1997, pp. 561-570	
		Diffie, W., et al., "New Directions in Cryptography", IEEE Transactions on Information Theory, 22(6):644-654, 1976	
		ElGamal, T., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, IT-31(4):469-472, 1985	
		Fiat, A., et al., "How to Prove Yourself: Practical Solutions to Identification and Signature Problems", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 186-194, Springer-Verlag, New York, 1987	
		Fujioka, A., et al., "A Practical Secret Voting Scheme for Large Scale Elections", Advances in Cryptology – AUSCRYPT 1992, Lecture Notes in Computer Science, pp. 244-251, Springer-Verlag, 1992	
		Gennaro, R., "Achieving independence efficiently and securely", Proceedings 14th ACM Symposium on Principles of Distributed Computing (PODC 1995), New York 1995	
		Iversen, K., "A Cryptographic Scheme for Computerized General Elections", CRYPTO 1991, pp. 405-419	
		Jan, Jin-Ke et al., "A Secure Electronic Voting Protocol with IC Cards", Elsevier Science Inc., New York, J. Systems Software 1997, 39:93-101	
		Mu, Yi et al., "Anonymous Secure E-Voting over a Network", Proceedings, Annual Computer Security Applications Conference, IEEE 1998, pp. 293-299	
		Odlyzko, A. M., "Discrete logarithms in finite fields and their cryptographic significance", Advances in Cryptology – EUROCRYPT 1984, Notes in Computer Science, Springer-Verlag, 1984	
		Park, C., et al., "Efficient Anonymous Channel and All/Nothing Election Scheme", Advances in Cryptology – EUROCRYPT 1993, Lecture Notes in Computer Science, pp. 248-259, Springer-Verlag, 1993	
		Pedersen, T., "A Threshold Cryptosystem without a Trusted Party", Advances in Cryptology – EUROCRYPT 1991, Lecture Notes in Computer Science, pp. 522-526, Springer-Verlag, 1991	
		Sako, K., et al, "Receipt-Free Mix-Type Voting Scheme – A practical solution to the implementation of a voting booth", EUROCRYPT 1995, pp. 393-403	
		Sako, K., et al., "Secure Voting Using Partially Compatible Homomorphisms", Advances in Cryptology – CRYPTO 1994, Lecture Notes in Computer Science, Springer-Verlag, 1994	
		Schnorr, C.P., "Efficient Signature Generation by Smart Cards", Journal of Cryptology, 4(3):161-174, 1991	
		Schoenmakers, B., "A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting", Advances in Cryptology – CRYPTO 1999, Lecture Notes in Computer Science, pp. 1-17, Springer-Verlag 1999	
		Shamir, A., "How to Share a Secret", Communications of the ACM, 22(11):612-613, 1979	

EXAMINER	DATE CONSIDERED

* EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).